RANDOM NUMBER GENERATOR

Patent number:	JP62109082
Publication date:	1987-05-20
Inventor:	OKAMOTO EIJI; NAKAMURA KATSUHIRO
Applicant:	NIPPON ELECTRIC CO
Classification:	
- international:	G09C1/00
- european:	
Application number:	JP19850250085 19851108
Priority number(s):	JP19850250085 19851108

Abstract not available for JP62109082

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　昭62-109082

⑤Int.Cl.⁴　識別記号　庁内整理番号　⑬公開　昭和62年(1987)5月20日
G 09 C 1/00　7368-5B

審査請求　未請求　発明の数 1　(全3頁)

⑭発明の名称　乱数発生器

⑳特　願　昭60-250085
㉒出　願　昭60(1985)11月8日

⑫発明者　岡本　栄司　東京都港区芝5丁目33番1号　日本電気株式会社内
⑫発明者　中村　勝洋　東京都港区芝5丁目33番1号　日本電気株式会社内
⑪出願人　日本電気株式会社　東京都港区芝5丁目33番1号
⑭代理人　弁理士　内原　晋

明細書

発明の名称　乱数発生器

特許請求の範囲

内部状態を更新しながら乱数を発生する乱数発生器において、あらかじめ定められたキーあるいは内部状態を表わすディジタルパターンを記憶する記憶手段と、前記ディジタルパターンに依存した複数あるいは単一のディジットを出力するパターン変換手段と、前記記憶手段に記憶されているディジタルパターンの少なくとも1つのディジットを前記パターン変換手段の出力するディジットと該ディジタルパターンの1つあるいは複数個のディジットとのM(Mは正整数)を法とする和に書き換え、該ディジタルパターンの少なくとも1つのディジットを該ディジタルパターンの少なくとも2つのディジットのMを法とする和に書き換える書き換え手段と、前記パターン変換手段が出力するディジットの一部あるいは全てを乱数として出力する乱数出力手段とから成ることを特徴とする乱数発生器。

発明の詳細な説明

(産業上の利用分野)

本発明は暗号通信に用いる乱数の発生に関する。

(従来技術とその問題点)

乱数発生方式としてよく用いられる方式はM系列発生器である。(M系列発生器については宮川、岩垂、今井著「符号理論」(昭晃堂、昭和54年版、128頁~129頁)を参照。しかし、M系列発生器は安全性が低い。即ち、シフトレジスタの段数の2倍の出力ビットがわかれば、他の出力は全て判明してしまう。そこでシフトレジスタの帰還部に非線形変換を用いた第2図の方式も用いられる。(例えばエージェン・パーク・プレス(Aegean Park Press)出版のシフト・レジスタ・シーケンセズ(Shift Register Sequences)に出ている。)図において201はシフトレジスタ、202は非線形変換である。しかしこのタイプでも安全性を高めるにはシフトレジスタの段数

を長くする必要があるが、長い場合にはシフトを十分に行なわないとシフトレジスタの中味が十分変化せず、従って安全性が低いという欠点があった。

(発明の目的)

本発明の目的は上記欠点を取除き、安全性の高い乱数発生器を与えることにある。

(発明の構成)

本発明の乱数発生器は、あらかじめ定められたキーあるいは内部状態を表わすディジタルパターンを記憶する記憶手段と前記ディジタルパターンに依存した複数あるいは単一のディジットを出力するパターン変換手段と、前記記憶手段に記憶されているディジタルパターンの少なくとも1つのディジットを前記パターン変換手段の出力するディジットと該ディジタルパターンの1つあるいは複数個のディジットとのM(Mは正整数)を法とする和に書き換え、該ディジタルパターンの少なくとも1つのディジットを該ディジタルパターンの少なくとも2つのディジットのMを法とする和に書き換える書き換え手段と、前記パターン変換手段が出力するディジットの1部あるいは全てを乱数として出力する乱数出力手段とから成ることを特徴とする乱数発生器である。

(本発明の作用・原理)

第1図は本発明の作用・原理を示すための図である。第2図と異なるのはシフトレジスタの帰還部であり、該帰還部によりシフトレジスタの段数が長くてもすぐにシフトレジスタの内容がランダム化される。なお、帰還部の結線としては例えばM系列発生器で用いた結線を用いる。

(実施例)

第3図は本発明の実施例を示すブロック図である。図において331は67段のシフトレジスタで、初期設定時にはキーパターンがはいる。301から322は16×1ビットROMである。ROM301から322には、各々4ビットずつ入力されるが、該4ビットをROMのアドレスとみなし、該アドレスに記憶されている1ビットを出力する。ROM322の出力は帰還されてシフトレジスタ331の最上位ビットと332の排他的論理和素子で排他的論理和(EOR)をとられて、シフトレジスタ331の最下位ビットに入力される。出力乱数はROM321の出力のうち8回に1度の出力となる。即ち、乱数1ビットを得るのに第3図を8回シフト動作させる。この8という数字は1例であり、1でもよい。301から322におけるROMに記憶するパターンはランダムなパターン、例えば物理的なランダムパターンである。このパターンをキーの1部とすることもできる。

以上の実施例において、乱数出力を321から得ているが、それぞれ322の出力として321を省略できる。またシフトレジスタ331はRAMで構成することができ、ROMも不揮発性RAMとすることができる。これらの変更は全て本発明の範囲に含まれる。

(発明の効果)

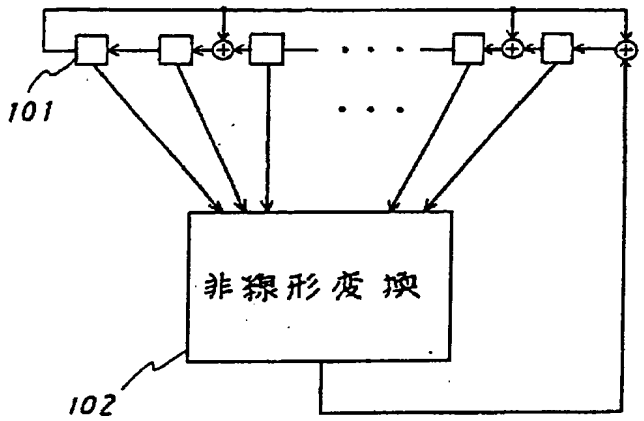
以上、詳細に説明したように、本発明を用いればシフトレジスタの中味がすぐにランダム化されるので、安全性の高い乱数発生器を得ることができ、暗号通信に用いて効果は大きい。

図面の簡単な説明

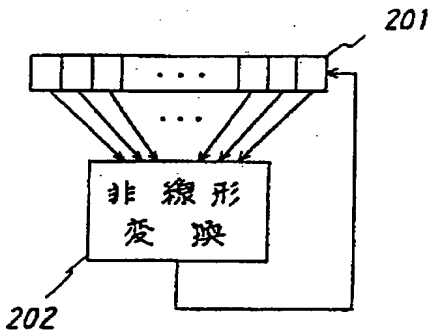
第1図は本発明の基本原理を示すためのブロック図、第2図は従来の乱数発生器を示すためのブロック図、第3図は本発明の実施例を示すための構成図である。図において、101,201,331はシフトレジスタ、102,202は非線形変換回路、332は排他的論理和素子、301~322はROM,342は各々表わす。

代理人 弁理士 内原

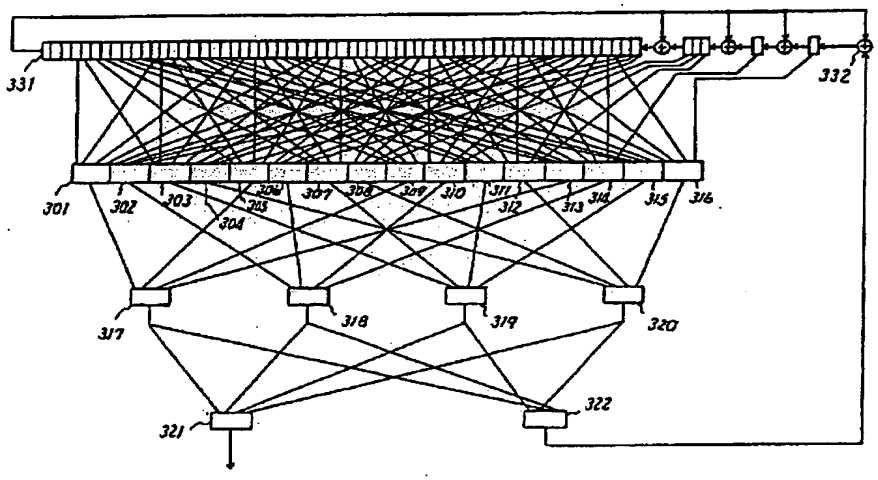
第　1　図


101
非線形変換
102

第　2　図


201
非線形
変換
202

第　3　図


331
332
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322